March 18, 2002

Consult With Private Firms on Cyber Security

By Rep. Mike Honda

Cyberterrorism is not only a threat, it is a reality. Since Sept. 11 the number of cyber attacks has skyrocketed, and the trend is expected to increase. Just as special operations teams have been used to test defenses at nuclear facilities, so too have "white hat" hackers demonstrated that seemingly "secure" networks containing sensitive information are vulnerable to attack.

Our nation's information network is an important part of our nation's critical infrastructure. Computer networks manage everything from air traffic control to energy transmission to emergency response to national defense. It has been said that just as airplanes have been used as weapons of mass destruction, our own computer networks could be used as "weapons of mass disruption" if hijacked by the wrong people. Unfortunately, our increased reliance on computers and computer networks raises the vulnerability of the nation's critical infrastructures to cyber attacks. The growing complexity and interconnectedness of this infrastructure means that disruption in one area may lead to disruption in others.

As Congress continues to address our nation's emerging security needs, it is essential that we understand that true national security means not only protecting people and places but data and networks, as well. Fortunately, the three fundamental elements for a cohesive approach to solving our cyber-security crisis already exist. First, strong, bicameral, bipartisan support for technology initiatives in a variety of security-related bills has created a framework of cooperation between political parties and both houses of Congress on technology issues. Second, new partnerships between all levels of government and the technology sector are gaining momentum, breaking down walls that previously separated the public sector and the technology sector. Third, Congress is coming to grips with the reality that training and educating a new generation of cyber-security experts is essential if we are to meet our present and future needs. These three principles must serve as the pillars of any sound national

cyber-security policy.

As a new Member representing Silicon Valley, I have been privileged to work with America's technology leaders and our Congressional leadership in formulating technology-driven solutions to national security issues in the aftermath of Sept. 11. One of the most important lessons I have learned this year is that technology knows no political party. After a contentious debate in the House, technology-savvy legislators such as Sen. Joe Lieberman (D-Conn.) and my colleague Rep. Jim Matheson (D-Utah) and I were able to work with Transportation and Infrastructure Chairman Don Young (R-Alaska), ranking member Jim Oberstar (D-Minn.) and the other conferees to develop a strong technology component in the final version of the airline security bill.

Another recent bipartisan technology victory was the 400-12 passage of the Cyber Security Research and Development Act (H.R. 3394), a bill introduced by Science Chairman Sherwood Boehlert (R-N.Y.) and ranking member Ralph Hall (D-Texas) that authorizes $880 million over five years for new programs to ensure that the United States is better prepared to prevent and combat terrorist attacks. The bill would create new cyber-security research centers, undergraduate program grants, community college grants and fellowships through the National Science Foundation. One provision of the Cyber Security Act, introduced by Rep. Brian Baird (D-Wash.), states that the National Institute of Standards and Technology will create new program grants for partnerships between academia and industry, new junior research positions and a new program to encourage senior researchers in other fields to work in computer security to help make up for the critical shortage of trained cyber-security personnel in the U.S. work force.

The third pillar of our cyber-security policy must build upon the positive dialogue that has developed between technology companies and all levels of government. In the past, ignorance on the part of some legislators and frustration on the part of some CEOs have hampered the emergence of productive partnerships between America's technology leaders and its policy leaders. But changing economic conditions and a new sense of patriotic purpose in Silicon Valley and technology corridors across the nation have engendered a new spirit of cooperation. Harnessing the energy and innovation of America's technology companies is essential if we are to educate Congress on our new cyber-security needs and the role that the latest cutting-edge applications can play in meeting those needs.

The most recent outcome of this new dialogue between government and technology companies is the United States Security Act (H.R. 3555), a sweeping counterterrorism measure that includes $2 billion in matching grants for state and local governments to improve information and security systems. While this is an important first step, the federal government must do more to fund state and local cyber-

security efforts.

Before this Congress is done with its work, I am hopeful that the leaders from both political parties will understand that the task of securing America's sensitive data and networks is larger in scope and complexity than the Y2K scenario. Throughout our history the public sector and private enterprise have worked together to face our nation's greatest challenges. It is incumbent upon the 107th Congress to build on this important legacy by passing a cohesive national cyber-security policy.

Rep. Mike Honda (D-Calif.) is a member of the Transportation and Infrastructure Committee.

Current Policy Briefing

Back To Top Home